Analysis of GPSR and its Relevant Attacks in Wireless Sensor Networks

Suraj Sharma[1], Sunil Kumar Panda[2], Rahul Ramteke[2] and Sanjay Kumar Jena[2]
[1] National Institute of Technology Rourkela, Odisha
Email: suraj.atnitrkl@gmail.com
[2] National Institute of Technology Rourkela, Odisha
Email: {sunil.panda.nit, rahulatnit, skjenanitrkl}@gmail.com

***Abstract*— Most of the routing protocols proposed for ad-hoc networks and sensor networks are not designed with security as a goal. Hence, many routing protocols are vulnerable to an attack by an adversary who can disrupt the network or harness valuable information from the network. Routing Protocols for wireless sensor networks are classified into three types depending on their network structure as Flat routing protocols, Hierarchical routing protocol and Geographic routing protocols. We mainly concentrate on location-based or geographic routing protocol like Greedy Perimeter Stateless Routing Protocol (GPSR). Sybil attack and Selective forwarding attack are the two attacks feasible in GPSR. These attacks are implemented in GPSR and their losses caused to the network are analysed.**

***Index Terms*—GPSR, Greedy, Perimeter, Selective forwarding attack, Sybil attack**

I. Introduction

Wireless Sensor Networks (WSN) is an interconnection of a large number of nodes deployed for monitoring the environment or system by means of measurement of environmental parameters like temperature, pressure, humidity. Sensor networks should also be adaptable to changing connectivity due to failure of node or introduction of new nodes. Sensor nodes being highly energy constrained pose serious challenges to the maintenance of highly scalable robust wireless network. The work is on thesis which is explored in this paper [10].

A. Routing Challenges

Scalability: A large number of sensor nodes should be deployed in sensing area and the routing scheme must be able to work with these huge number of sensor nodes.
Fault tolerance: Failure of certain nodes will affect the overall routing scheme. So formation of new links should be accomplished.
Coverage: Wireless Sensor Networks must be deployed in a large area to ensure more accuracy of the events occurring in the environment.
Heterogeneity: Some sensor nodes differ in their technical design, data routing becomes little problem as sensing rate is different for different sensors.

B. Classification of Routing Protocols

Routing protocols [8] are responsible for routing data packets from source node to the destination node. Depending on the behavior for establishment of paths from source to destination routing protocols can be classified as proactive, reactive, hybrid. Routing protocols can also be classified on the basis of network structure as Flat Network Routing, Hierarchical Network Routing and Location based routing [8].

The rest of the report is organized as follows. Section II describes the Greedy perimeter stateless routing protocol (GPSR). Section III discusses the relevant attacks on GPSR. Section IV gives the implementation detail of GPSR and Selective, Sybil attack simulation over GPSR, followed by conclusion and lists the future work.

II. Greedy Perimeter Stateless Routing Protocol (GPSR)

Greedy Perimeter Stateless Routing (GPSR) [1] is a geographic or location based routing protocol that uses the geographic positions of routers and packets destination to make packet forwarding decision. Each node in a sensor network keeps track of the location of its immediate neighbors by using a simple beaconing algorithm. Periodically each node transmits a beacon to its immediate neighbors containing its own identifier and position [9]. In GPSR each node needs the propagation of topology information for all those nodes which are single hop distance. Thus the state required is minimum. As the name suggests GPSR routes the data packets in greedy mode. Greedy forwarding is used throughout the network whenever possible but in the regions where greedy forwarding fails perimeter forwarding is used.

A. Greedy Forwarding

To forward a packet to its neighbor a source must know the geographic location of the destination. This information can be obtained by a location server like GPS. A packet can then be routed towards the destination in the greedy mode. In a greedy mode a node selects the next node as that neighbor which is geographically closest to the destination. Thus GPSR [2] can save much amount of energy and can scale to large number of nodes in Wireless Sensor Network.

B. Perimeter Forwarding

There may be topology which requires a data packet to move temporarily away from the destination. When a node encounters a void then it switches from greedy to perimeter mode [3]. A node selects the next node according to the righthand rule and the packet follows the path along the perimeter of the void towards the destination and the packet is said to enter into the perimeter mode [1].

DOI: 01.IJNS.03.01.116

C. Right Hand Rule

The right hand rule in graphs is used to route the packet whenever the packet encounters a void. Thus right hand rule says that when arriving at node x from node y, the next edge traversed will be the next sequential counter-clockwise about y the edge (x, y).

D. Planarized graphs

Planarized graphs are used to remove cross links in the network. A graph is said to be planar if no two edges cross. The Relative Neighborhood Graph (RNG) and Gabriel Graph (GG) [1] are two long known planar graphs. The RNG or GG algorithm yields a network with no cross edges or crossing links.

Relative Neighborhood Graph (RNG):

The RNG can be defined as follows: An edge (u, v) will exist between the vertices of u and v, if the distance between d (u, v) is always less than or equal to the distance between the vertex *w*, and whichever among *u* and *v* is farther away from *v*. In equation form [1]:

$$\forall w = u, v: d(u, v) < max\ [d(u, w), d(v, w)]$$

Gabriel Graph (GG):

Gabriel Graph [1] can be defined as follows: An edge (*u*, *v*) may exist between vertices u and *v* if no other vertex w is present within the circle whose diameter is *uv*. In equation form [1]:

$$\forall w = u, v: d^2(u, v) \leq [d^2(u, w) + d^2(v, w)]$$

The full Greedy Perimeter Stateless Routing algorithm combines greedy forwarding on the full network graph with perimeter forwarding on the planarized network graph where greedy forwarding is not possible.

III. Attacks On Geographical Routing Protocols

Greedy Perimeter Stateless Routing Protocol is robust and efficient for the applications of Wireless Sensor Network but it was not designed with security as a goal. The attacks in sensor networks can be mainly distinguished as outsider attacks and the insider attacks [5]. In outsider attack the attacker has no special access to the sensor network whereas in an insider attack the attacker can access the sensor network and model an attack by using compromised node to run malicious code.

A. Selective Forwarding Attack

In a wireless sensor network some nodes may drop all the packets received for routing to the destination. A more subtle form of attack is realized when an adversary does not drop all the packets but selectively forwards few packets while dropping all the other packets. Selective forwarding [4] can cause no reporting or late reporting of an event in Wireless Sensor Network. We have simulated selective forwarding attack on GPSR for wireless sensor network and measured the loss incurred by the network

B. Sybil Attack

In a Sybil attack [4, 6] an adversary node presents multiple identities to other nodes in the network to use the services offered by the network. In GPSR for wireless sensor network the nodes exchange their own and also their other neighbor's location coordinates with their neighboring nodes by sending beacons at regular intervals. An adversary node in a network can initiate the Sybil attack by sending false location information.

C. Bogus Routing

This is the most common type of attack which can take place in Geographic Routing Protocol. Main motive of this attack is to modify or alter the routing information which is commonly exchanged between two neighbor nodes. By spoofing the routing information adversaries becomes capable of creating routing loops.

IV. Implementation And Results

We have developed and integrated GPSR routing protocol [7] into Qualnet5.0.2. We have also simulated Greedy Perimeter Stateless Routing Protocol (GPSR) [7] in QualNet5.0.2. Further we have implemented Selective forwarding attack and Sybil attack over GPSR to analyze the losses incurred by the wireless sensor network. The results obtained from simulation of GPSR help us to measure the loss caused by the attacks.

A. Implementation of GPSR

A Wireless sensor network consisting of 17 nodes is used for simulation. Node 15 acts a source or CBR client and Node 9 acts as a destination or CBR server. All the nodes are set to use GPSR as a routing protocol. An event has occurred near node 15 which acts as a source and the event has to be reported to node 9 which acts as a base station. To find the coordinates of neighboring nodes, each node sends beacons at regular intervals. A beacon packet consists of the location of the node sending the beacon as well as their neighbor's location. The total number of beacon sent during simulation by each node is 68. A node can receive beacons from more than one neighbor. Total number of beacons sent and received during simulation is shown in Figure 1 for each node.

Once the location of neighboring nodes is known packets can be routed towards the destination in greedy mode. As shown in Figure 2, the number of greedy forwards by nodes 3, 5, 14 and 15 are maximum as their respective neighbors are closer to the destination. Conversely, as shown in Figure 3, nodes 9, 10, 14 have their respective neighbor's farther from the destination. Thus they have maximum perimeter forwards. Greedy forwards and perimeter forwards are the number of packets forwarded by nodes in greedy and perimeter modes respectively. As the packets are routed towards the destination they are switched from greedy mode to perimeter mode when they encounter a void and switchback to the greedy mode after covering the void several times until destination is reached. In the simulation the number of packet dropped for each node is measured to be zero.

DOI: 01.IJNS.03.01.116

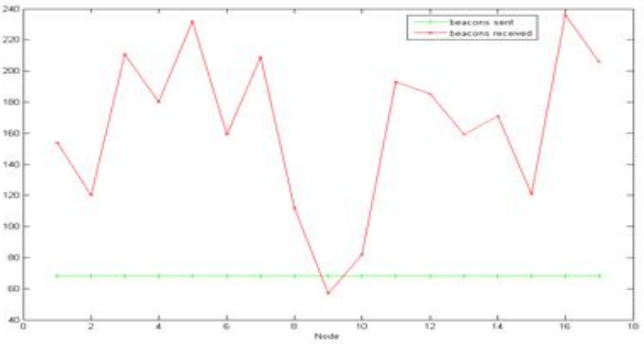

Figure.1. Total number of beacons sent and received.

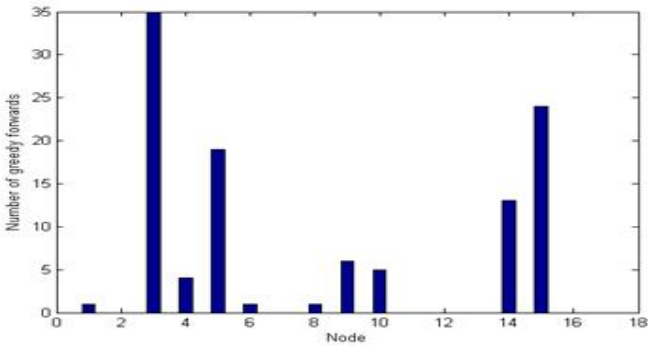

Figure.2. GPSR greedy forwards.

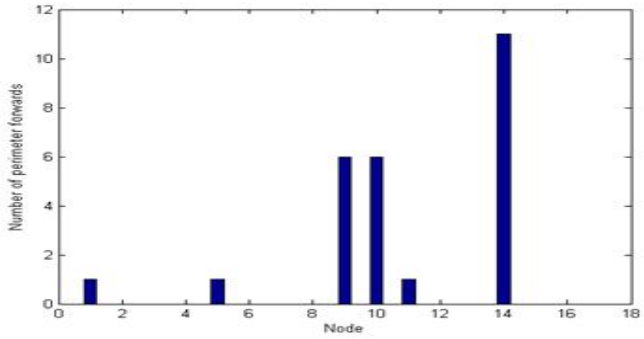

Figure 3. GPSR perimeter forwards.

B. Implementation of Selective forwarding attack over GPSR

The example scenario of section III is used to implement selective forwarding attack over GPSR. In our sample scenario we have selected node 4, 7 and 10 as malicious nodes to launch selective forwarding attack over GPSR. The selective forwarding attack does not alter the number of beacons sent and beacons received .Thus the total number of beacons sent and beacons received remains same as in GPSR as inferred from the Figure 4.

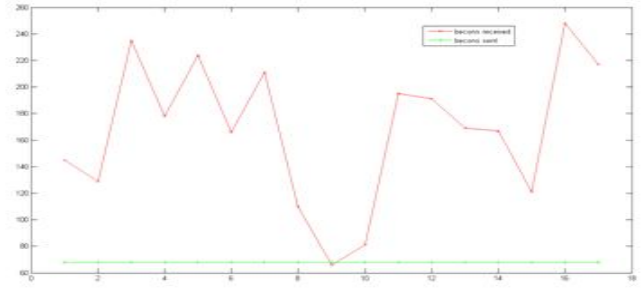

Figure.4. Beacon sent and Beacon received for Selective Forwarding attack

Similarly, selective forwarding attack does not much alter the greedy forwards and the perimeter forwards of the nodes. The smaller variation can be observed from Figure 5, 6 which is caused to cope the number of packets lost in the routing path. The number of greedy forwards for node 11 and node 13 were 0 each in GPSR whereas in implementation of selective forwarding attack over GPSR it is found to be increased by 1 each as shown in Figure 5.

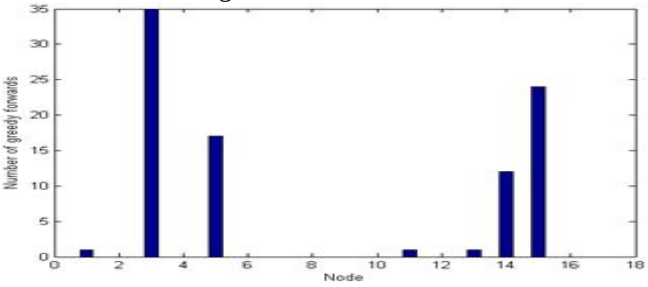

Figure.5. Number of greedy forwards in GPSR with Selective forwarding attack.

The malicious nodes now drop most of the packets received and selectively forward the packet. As can be seen from Figure 7 the number of packet dropped for node 4 and node 10 is very high as compared to GPSR. Node 7 being a malicious node has zero number of packets dropped as packets are not routed through node 7. The loss of packets may lead to loss of an event being reported to the destination.

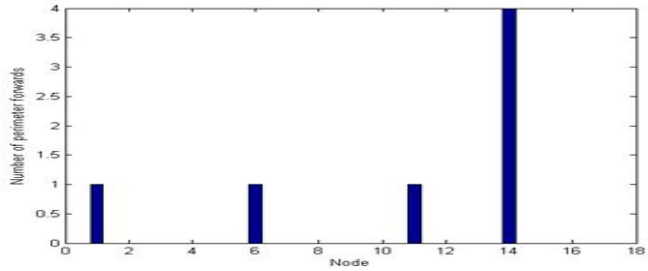

Figure.6. Number of perimeter forwards in GPSR with Selective forwarding attack.

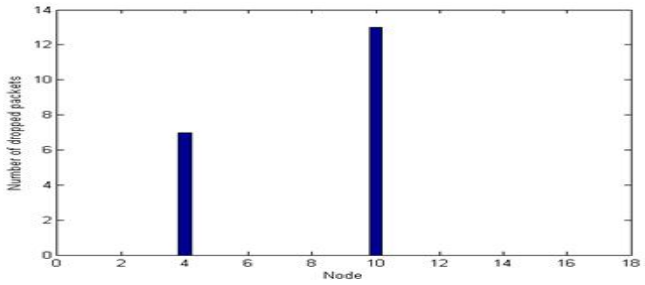

Figure.7. Number of dropped packets in GPSR with Selective forwarding attack.

C. Implementation of Sybil attack over GPSR

The example scenario of section III is used to implement Sybil attack over GPSR. In our sample scenario we have selected node 1, 3 and 14 as malicious nodes to launch Sybil attack over GPSR. Sybil attack is launched by the malicious nodes by sending more number of beacons than the normal nodes to falsely advertise multiple locations. In our case each malicious node advertises four more false locations.Thus the number of beacons sent for Sybil nodes are approximately four times the normal nodes as can be seen from Figure 8.

DOI: 01.IJNS.03.01. 116

This results in increase in the number of beacons received by other nodes and the number of fake identities in the network.The Sybil attack alters the number of beacons sent and beacons received .Thus the total changed number of beacons sent and beacons received leads to small variations in network in terms of greedy forwards, perimeter forwards etc. The smaller variation can be observed from Figure 9, 10 which is caused to cope the changed number of beacons and advertisement of multiple locations of a Sybil node in the routing path. The number of greedy forwards for node 8 and node 13 were 1 and 0 respectively in GPSR whereas in implementation of Sybil attack over GPSR it is found to be increased by 1 for node 13 and decreased by 1 for node 8 respectively as shown in Figure 9.

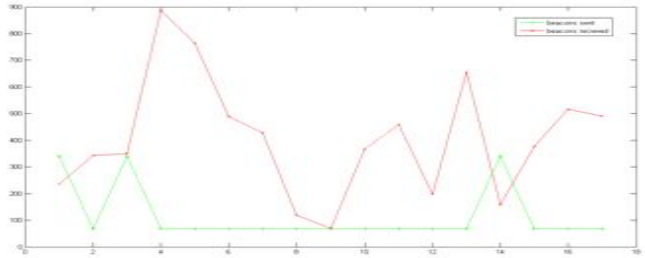

Figure.8. Beacon sent and Beacon received for Sybil attack over GPSR.

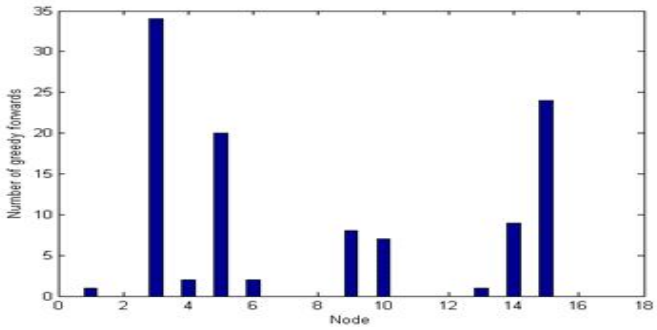

Figure.9. Greedy forwards for Sybil attack over GPSR.

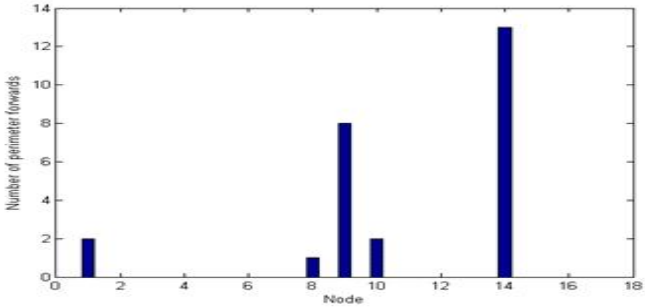

Figure.10. Perimeter forwards for Sybil attack over GPSR.

Conclusions

GPSR was simulated for wireless sensor network and the packets were found to switch from greedy mode to perimeter mode to encounter a void in the routing path. Selective forwarding attack was simulated over GPSR and it was found that the packets dropped for malicious node has increased as compared to that in GPSR.This may lead to an event being unreported to base station. Sybil attack was implemented and it was found that malicious node advertising multiple geographic locations sends more number of beacons to their neighbors' as in comparison with GPSR, tends to alter the routes of packets and wastage of network resources.

References

[1] Brad Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," *Proceedings of the 6th annual international conference on Mobile computing and networking New York, NY, USA*, pp. 243–254, 2000.

[2] D. Estrin, Y. Xu and J. Heidemann, "Geography-informed energy conservation for ad-hoc routing," *In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 70–84, 2001.

[3] F. Kuhn, R. Wattenhofer, and A. Zollinger, "Worst-case optimal and average-case efficient geometric ad-hoc routing," *In Proceedings of the 4th ACM International Conference on Mobile Computing and Networking*, pp. 267–278, 2003.

[4] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *In First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113 –127, 2002.

[5] Haowen Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks," *In Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pp. 197–213, May 2003.

[6] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis and defenses," *In Proceedings of the 3rd international symposium on Information processing in sensor networks*, pp. 259–268, April 2004.

[7] Paolo Lutterotti, Giovanni Pau and UCLA, "GPSR: greedy perimeter stateless routing," *Contributed model for Vehicular Networks*, June 2010.

[8] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, pp. 6–28, December 2004.

[9] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks," *Technical report, UCLA Computer Science Department*, 2001.

[10] S. K. Panda, R. Ramteke and S. K. Jena' "Attacks on Geographic Routing Protocols for Wireless Sensor Network," *Thesis NIT Rourkela, Orissa, India*, 2011.

DOI: 01.IJNS.03.01.116